I. General Remarks Concerning This Response

Claims 1-25 are currently pending in the present application. No claims have been amended, added, or canceled in this response. Reconsideration of the claims is respectfully requested.

II. Summary of Present Invention

A method and a system is presented for managing attribute certificates. A target service within a distributed data processing system receives an attribute certificate from a client. A locator is retrieved from the attribute certificate; the locator identifies a location of a public key certificate of an issuing authority for the attribute certificate. The public key certificate of the issuing authority for the attribute certificate is then retrieved from the specified location. The attribute certificate is then verified by using the public key certificate of the issuing authority for the attribute certificate. The client is then authorized to have access to the controlled resources in the target service in accordance with authorization attributes in the attribute certificate.

An extension within an attribute certificate, called a distributed trust path locator, allows an attribute certificate to be physically disassociated from its supporting public key certificates while remaining logically associated with its supporting public key certificates. The user's attribute certificate and its supporting public key certificates allows any server using an attribute certificate to locate and retrieve the public key certificate of the user and of the AC-issuing authority. The user is not required to communicate his/her public key certificate to a target service. In addition, configuring the target service to accept attribute certificates does not require the deployment of a public key certificate for every AC-issuing authority.

III. 35 U.S.C. § 103(a)—Obviousness—*AAPA in view of Zubeldia and Grimmer*

The Office action has rejected claims 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, and 23 under 35 U.S.C. § 103(a) as unpatentable over Applicant's Admitted Prior Art (AAPA) in view of Zubeldia, "Digital certification system", EPO Patent Application Publication EP 0869637 A2, filed 04/01/1998, published 10/08/1998, and further in view of Grimmer, "Method and apparatus for retrieving X.509 certificates from an X.500 directory", U.S. Patent Number 5,774,552, filed 12/13/1995, issued 06/30/1998. This rejection is traversed.

The Office action contains a common rejection of independent claims 1, 5, 7, 9, 13, 15, 17, 21, and, 23, which includes all of the pending independent claims of the present patent application except independent claim 25. The independent claims primarily differ with respect to the perspective of an entity that acts on an attribute certificate; for example, some of the claims are directed to a method that is performed by a server, whereas some of the claims are directed to a method that is performed by a client. Since the Office action has focused on claim 1 as representative of these independent claims, Applicant provides a rebuttal of the rejection with respect to claim 1 while asserting that the arguments that are provided in support of the patentability of independent claim 1 are applicable to independent claims 5, 7, 9, 13, 15, 17, 21, and, 23.

It should be noted that this rejection relies upon Grimmer. Apparently, Grimmer is relied upon merely for its disclosure of storing digital certificates in a repository that allows compliance with the X.509 standard, which is a feature that is not recited within the independent claims. It is unclear why Grimmer is included at this particular location within the Office action. Hence, Applicant asserts that Grimmer is irrelevant with respect to the main obviousness argument.

All of the pending independent claims have been rejected, at least in part, over the disclosure in Zubeldia; each of the independent claims has at least one common element against which the Office action applies the teachings of Zubeldia. However, Applicant asserts that Zubeldia does not disclose the claimed feature for which the Office action relies on Zubeldia as disclosing, notwithstanding the arguments in the Office action, thereby causing the rejection to be deficient. In addition, Applicant makes other arguments to support Applicant's contention that the rejection is deficient for failing to present a *prima facie* case of obviousness.

More specifically, the Office action addresses the first, fourth, and fifth elements of claim 1 by referencing Applicant's Admitted Prior Art (AAPA); Applicant does not dispute this portion of the argument in the rejection. However, the Office action then addresses the second and third elements of claim 1 by referencing Zubeldia. Independent claim 1 reads as follows:

> 1. A method for authorizing access to controlled resources within a distributed data processing system, the method comprising:
>
> receiving an attribute certificate from a client at a host within the distributed data processing system;
>
> extracting a first locator from the attribute certificate, wherein the first locator identifies a location of a public key certificate of an issuing authority for the attribute certificate;
>
> retrieving the public key certificate of the issuing authority for the attribute certificate;
>
> verifying the attribute certificate using the public key certificate of the issuing authority for the attribute certificate; and
>
> authorizing the client to have access to the controlled resources in accordance with authorization attributes stored in the attribute certificate.

The rejection admits that AAPA does not disclose the second and third elements of claim 1 by stating on page 3 of the Office action that "AAPA does not explicitly disclose ..." these claim elements. The rejection then continues by discussing Zubeldia.

As an initial point, Applicant notes that the portions of the rejection that discuss Zubeldia are written as if the claim language merely recites operations on a digital certificate. However, this is not the case. The present invention is particularly directed to novel features with respect to a special type of digital certificate--an attribute certificate. By disregarding the fact that the present invention is directed to operations on an attribute certificate, the rejection presents an self-contradicting argument as to why one having ordinary skill in the art would have been motivated to modify the prior art to reach the present invention, as discussed in more detail further below.

The rejection argues that the second and third elements of claim 1 are disclosed by Zubeldia by stating:

> However, Zubeldia discloses using certificate index to retrieve certificate information used for authentication from repository (Zubeldia: page 4, line 33 - page 5 line 8). It would have been obvious to one having ordinary skill in the art to use the certificate index to retrieve information required for authenticating the digital certificate. Therefore, it would have been obvious to one having ordinary skill in the art to combine the teachings of Zubeldia within the system of AAPA because it allows more efficient and flexible digital certification by storing necessary information for authenticating the certificate in a central repository so that it is easy to change attributes in the certificate.

The Office action is correct that Zubeldia discloses the feature of "using certificate index to retrieve certificate information used for authentication from repository" as stated by the rejection. Zubeldia states the following on page 4, lines 33-57:

> The present invention provides a digital certification system which allows a user to add information to a digital certificate without requiring the re-issuance of the digital certificate and the invalidating of all distributed copies of the previous certificate. The invention comprises a digital certificate and the associated computer system and procedure which support its usage.

> The digital certificate of the present invention is split into two components. One component (the "certificate index") is distributed to the user and the public. The other component (the "certificate information") is maintained by the certification authority in a publicly available trusted repository.
>
> In one embodiment, a certification authority generates a unique user ID for an applicant for a digital certificate. The certification authority then issues a digital certificate containing, in the certificate index, the unique user ID, the user's public key, and the user's name. Unlike in the prior art, in the present invention, additional certificate information (such as, for example, the user's E-mail address, or biometric information) is excluded from the digital certificate index. Instead, such additional certificate information is maintained by the certification authority in a publicly available trusted repository.
>
> Access to the additional certificate information is obtained through the unique user ID in the certificate index. Instead of linking a public key, a user name, and the additional information, the digital certificate of the present invention links a public key with an unchanging user ID, which allows access to the additional certificate information. The present invention thus allows the certification authority to change the additional certificate information at the request of the user without requiring issuance of a new certificate.

In the system that is disclosed in Zubeldia, the certificate information that is stored in the publicly available trusted repository contains the certificate authority's signature over the certificate information; on page 7, lines 52-55, Zubeldia states that "[t]he certificate information 600 includes ... a CA's digital signature of the certificate information 690". Hence, it is correct for the rejection to state that Zubeldia discloses the feature of "using certificate index to retrieve certificate information used for authentication from repository" because the certificate authority's signature would be verified as part of the process of authenticating the type of digital certificate that is disclosed by Zubeldia.

However, Zubeldia states that following on page 8, lines 45-48 (emphasis added):

> In step 1103, the receiver verifies the authenticity of the digital certificate index obtained in step 1102 by checking the digital signature of the issuing CA on the digital certificate. For example, if the digital certificate index has a form shown in Figure 9, **the receiver decrypts CA's digital signature 900 using the CA's public key (to which the receiver has access)**, and obtains a first decrypted message digest.

Although Zubeldia describes a novel type of digital certificate, an entity that needs to verify or authenticate an instance of the novel type of digital certificate is responsible for obtaining a copy of the public key certificate of the certificate authority that issued the instance of the novel type of digital certificate that is to be verified. This responsibility also exists in a similar situation with a standard X.509 digital certificate; in other words, in a typical system, the entity that needs to verify or authenticate the X.509 digital certificate is responsible for obtaining a copy of the public key certificate of the certificate authority that issued the X.509 digital certificate that is to be verified.

Thus, Zubeldia does not disclose anything novel with respect to the need of the verifier of a digital certificate to have access to a copy of the certificate authority's public key certificate in some manner. In a typical X.509-compliant system, the verifier may obtain a copy of the certificate authority's public key certificate in two different ways. First, the verifier may have access to a copy of the certificate authority's public key certificate because the verifier received it along with the digital certificate that is to be verified; for example, the verifier may be a service that receives a copy of the public key certificate of a customer along with a copy of the public key certificate of the certificate authority that issued the customer's digital certificate. Second, the verifier may know of a publicly available certificate repository to which the verifier has access in order to retrieve a copy of the certificate

authority's public key certificate after receiving a copy of the public key certificate of a customer.

In contrast, the present invention discloses that a verifier of an attribute certificate has access to a copy of the public key certificate of the issuing authority of the attribute certificate (the certificate authority that issued the attribute certificate) because it extracts from the attribute certificate a locator that identifies a particular storage location for the public key certificate of the issuing authority. More specifically, independent claim 1 recites:

> ... extracting a first locator from the attribute certificate, wherein the first locator identifies a location of a public key certificate of an issuing authority for the attribute certificate;
>
> retrieving the public key certificate of the issuing authority for the attribute certificate; ...

There is nothing equivalent nor analogous in Zubeldia to this claimed feature of the present invention as recited within the second and third elements of claim 1. Zubeldia discloses a locator, i.e. a "certificate index", at which to find the "certificate information", which includes information that would be stored within a typical X.509. However, Zubeldia does not disclose nor suggest that the "certificate information" does include or could include the digital certificates that are needed to verify the "certificate index" and the "certificate information". Applicant asserts that the secondary prior art reference, Zubeldia, does not disclose the claimed feature for which the rejection relies on Zubeldia as disclosing in order to support the rejection's argument. Hence, Applicant asserts that the rejection fails to provide *prima facie* case of obviousness against the claimed present invention.

Moreover, Zubeldia teaches away from the present invention. Zubeldia does not disclose nor suggest that the "certificate information" includes a copy of the public key certificate of the certificate authority that issued the digital certificate because

this feature of the present invention would contradict the purpose of the novel features in Zubeldia. The purpose of the data items within the "certificate information" is related multiple times throughout Zubeldia, e.g., which states on page 7, lines 8-10: "Changeable user information, instead of being included in the certificate index, is maintained at a location indicated by the unique user ID." In its summary section, Zubeldia teaches that the "certificate information" includes "additional certificate information" that "allows the certification authority to change the additional certificate information at the request of the user without requiring issuance of a new certificate". The public key certificate of the certificate authority that issues the certificate does not fit into the same category of information as "changeable user information". Thus, Zubeldia teaches away from its inclusion in the "certificate information" in contradiction to the argument in the rejection. Since Zubeldia teaches away from the claimed features of the present invention, Applicant asserts that the rejection fails to provide *prima facie* case of obviousness against the claimed present invention.

Furthermore, the motivational statement in the obviousness rejection of claim 1 is misleading for multiple reasons. First, the rejection states that "[i]t would have been obvious to one having ordinary skill in the art to use the certificate index to retrieve information required for authenticating the digital certificate." However, it is confusing why the rejection does not further discuss why this particular statement is relevant. As discussed above, it is correct to state that Zubeldia discloses using a certificate index to retrieve information that is required for authenticating the digital certificate, but the rejection does not follow this statement with any other statements concerning its importance. Second, the rejection states:

> It would have been obvious to one having ordinary skill in the art to combine the teachings of Zubeldia within the system of AAPA because it allows more efficient and flexible digital certification by storing necessary information for authenticating the certificate in a central repository so that it is easy to change attributes in the certificate.

In other words, the hypothetical system that combines Applicant's Admitted Prior Art (AAPA) and Zubeldia would supposedly provide the advantage of "storing necessary information for authenticating the certificate in a central repository so that it is easy to change attributes in the certificate." However, given the fact that digital certificates were commonly stored in directories, one could argue that AAPA already discloses "storing necessary information for authenticating the certificate in a central repository", thereby partly negating the supposed motivation in modifying a system that is implemented in accordance with AAPA. Moreover, one of the purposes of an attribute certificate as disclosed by AAPA is that one wants to bind the user's attributes in a digital certificate such that those attributes cannot be modified without obtaining a new attribute certificate, thereby also negating the supposed motivation in modifying a system that is implemented in accordance with AAPA. Applicant asserts that one of ordinary skill in the art would not have been motivated by the reasons that are provided within the rejection to modify the teachings in AAPA; hence, the obviousness rejection fails to provide *prima facie* case of obviousness against the claimed present invention.

More specifically, Applicant asserts that modifying AAPA to include teachings of Zubeldia as argued in the rejection would completely change the principle of operation of AAPA. As noted above, an X.509 attribute certificate as disclosed by AAPA is a digital certificate that ensures that a user's attribute information within the digital certificate remains unchanged. One wants to bind the user's attributes in a digital certificate such that those attributes cannot be modified without obtaining a

new attribute certificate. The present invention provides a novel feature of including "a locator" in an attribute certificate such that the locator identifies a storage location of a copy of the public key certificate of the certificate authority that issued the attribute certificate; the user's attribute information remains bound within the attribute certificate.

In contrast, Zubeldia discloses the use of a "certificate index" that allows the user's information ("certificate information") to be located in a repository such that the information in the repository can be changed more easily without having to issue a new digital certificate. At most, a hypothetical combination of AAPA and Zubeldia as argued by the rejection using the suggested advantages of Zubeldia would result in a system in which the user's attribute information from the attribute certificate was stored in a repository. However, this modification would negate the purpose of using an attribute certificate at all. If the user's attribute information could be easily changed within the repository, then a third party, such as an e-commerce web site, could not depend on the user's attribute information for performing authorization operations. In other words, the security advantages of using an attribute certificate would be lost. As stated in stated in MPEP § 2143.01:

> If the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims prima facie obvious. *In re Ratti*, 270 F.2d 810, 123 USPQ 349 (CCPA 1959).

Applicant asserts that one of ordinary skill in the art would not have been motivated by the reasons that are provided within the rejection to modify the teachings in AAPA; hence, the obviousness rejection fails to provide *prima facie* case of obviousness against the claimed present invention.

Dependent claims 3, 11, and 19 recite further limitations. Since the dependent claims incorporate the features of the independent claims, the rejections are similarly deficient with respect to the dependent claims for the same reasons that were argued above with respect to the independent claims.

Examiner bears the burden of establishing a *prima facie* case of obviousness

The examiner bears the burden of establishing a *prima facie* case of obviousness based on the prior art when rejecting claims under 35 U.S.C. § 103. *In re Fritch*, 972 F.2d 1260, 23 U.S.P.Q.2d 1780 (Fed. Cir. 1992). Only when a *prima facie* case of obviousness is established does the burden shift to the applicant to produce evidence of nonobviousness. *In re Oetiker*, 977 F.2d 1443, 1445, 24 U.S.P.Q.2d 1443, 1444 (Fed. Cir. 1992); *In re Rijckaert*, 9 F.3d 1531, 1532, 28 U.S.P.Q.2d 1955, 1956 (Fed. Cir. 1993). If the Patent Office does not produce a *prima facie* case of unpatentability, then without more the applicant is entitled to grant of a patent. *In re Oetiker*, 977 F.2d 1443, 1445, 24 U.S.P.Q.2d 1443, 1444 (Fed. Cir. 1992); *In re Grabiak*, 769 F.2d 729, 733, 226 U.S.P.Q. 870, 873 (Fed. Cir. 1985). In response to an assertion of obviousness by the Patent Office, the applicant may attack the Patent Office's *prima facie* determination as improperly made out, present objective evidence tending to support a conclusion of nonobviousness, or both. *In re Fritch*, 972 F.2d 1260, 1265, 23 U.S.P.Q.2d 1780, 1783 (Fed. Cir. 1992).

AAPA and Zubeldia clearly fail to disclose at least one feature of the present invention as recited within each independent claim, notwithstanding the arguments presented by the Office action, thereby rendering AAPA and Zubeldia incapable of being used as primary and secondary references as argued by the current rejection. Moreover, a hypothetical combination of AAPA and Zubeldia would also fail to reach the claimed invention of

the present patent application. As should be recognized, because both the primary and secondary references in the rejection fail to disclose the claimed features against which the references were applied, and because the references fail to be combinable to produce these claimed features, the rejection fails to fulfill the requirements of a proper obviousness argument.

With respect to the claims of the present patent application, Applicant respectfully submits that it would not have been obvious for one having ordinary skill in the art to have used the applied prior art references to reach the claimed invention. Hence, a rejection of the claims cannot be based upon the cited prior art to establish a *prima facie* case of obviousness. Therefore, a rejection of the claims under 35 U.S.C. § 103(a) has been shown to be insupportable in view of the cited prior art, and the claims are patentable over the applied references. Applicant respectfully requests the withdrawal of the rejection of the claims.

IV. 35 U.S.C. § 103(a)–Obviousness–*AAPA in view of Zubeldia, Grimmer, Kent, and de Silva*

The Office action has rejected claims 2, 6, 8, 10, 14, 16, 18, 22, and 24 under 35 U.S.C. § 103(a) as unpatentable over Applicant's Admitted Prior Art (AAPA) in view of Zubeldia, Grimmer, and further in view of Kent, "Method and apparatus for supporting authorities in a public key infrastructure", U.S. Patent Number 6,671,804, filed 01/01/1999, issued on 12/30/2003, and de Silva et al., "Digital certificate cross-referencing", U.S. Patent Number 6,615,347 B1, filed 06/30/1998, issued 09/02/2003. This rejection is traversed.

The Office action contains a common rejection of dependent claims 2, 6, 8, 10, 14, 16, 18, 22, and 24, which includes many of the pending dependent claims of the present patent application. These dependent claims primarily differ with

respect to the perspective of an entity that acts on an attribute certificate; for example, some of the claims are directed to a method that is performed by a server, whereas some of the claims are directed to a method that is performed by a client. Since the Office action has focused on claim 2 as representative of these dependent claims, Applicant provides a rebuttal of the rejection with respect to claim 2 while asserting that the arguments that are provided in support of the patentability of dependent claim 2 are applicable to dependent claims 6, 8, 10, 14, 16, 18, 22, and 24.

The Office action on page 4 states that "AAPA as modified does not explicitly disclose ..." the first element of claim 2. Dependent claim 2 reads:

> 2. The method of claim 1 further comprising:
> extracting a second locator from the attribute certificate, wherein the second locator identifies a location of a public key certificate of a holder of the attribute certificate;
> retrieving the public key certificate of the holder of the attribute certificate;
> authenticating the holder using the public key certificate of the holder.

The rejection then states: "However, Kent discloses the attribute certificate has a pointer that binds attribute certificate with the user's public key certificate (Kent: column 1, lines 36-39)." The cited portion of Kent reads: "Other forms of certificates, called attribute certificates, bind data other than a public key to a user's name, and associate the user's public key through a pointer to the user's public key certificate."

Applicant asserts that Kent does not disclose anything more than Applicant's Admitted Prior Art (AAPA). In the specification of the present patent application, Applicant states:

> In the prior art, the user sends both his/her attribute certificate and public key certificate to the target service. The two certificates are linked together in some manner; in the X.509 specification, the "Holder" field in the attribute certificate contains linking information for

the public key certificate, such as the identity of the public key certificate's issuing authority and the serial number of the holder's public key certificate.

Applicant asserts that the use of the term "pointer" in Kent is equivalent to the use of the term "linking information" in Applicant's own specification in which Applicant discussed the prior art, particularly given the fact that Kent discusses the features of a typical X.509 attribute certificate in its background section without discussing any novel features with respect to attribute certificates.

More importantly, Kent does not disclose the first element of claim 2, which specifically recites that the attribute certificate of the present invention includes a locator that identifies "a location of a public key certificate of a holder of the attribute certificate". In other words, the attribute certificate of the present invention does not merely identify, as is done in the prior art and as is done in Kent, the appropriate public key certificate that is associated with the attribute certificate. Since Kent does not disclose the claimed feature, notwithstanding the argument in the rejection, Applicant asserts that the rejection is deficient for not presenting a *prima facie* case of obviousness with respect to dependent claim 2.

The Office action on page 4 also states that "AAPA as modified does not explicitly disclose that there are two locators stored in the digital certificates." The rejection then states: "However, de Silva discloses storing a plurality of related certificates in the extension field of a certificate (de Silva: figure 3 and column 5 lines 15-41 and column 6 line 56-column 7 line 5)." Assuming *arguendo* that de Silva et al. discloses the feature as argued by the rejection, Applicant notes that Kent fails to disclose the second element of claim 2, i.e. "a second locator from the attribute certificate, wherein the second locator identifies a location of a public key certificate of a holder of the attribute certificate". Since Kent does not

disclose a first locator, it is irrelevant whether an argument for the inclusion of two locators can be made based on the disclosure of de Silva et al. as argued by the rejection. Since Kent does not disclose the claimed feature, notwithstanding the argument in the rejection, it is not possible to combine the teachings of Kent and de Silva et al. to reach the present patent application, notwithstanding the argument in the rejection to the contrary. Again, Applicant asserts that the rejection is deficient for not presenting a *prima facie* case of obviousness with respect to dependent claim 2.

With respect to claims 2, 6, 8, 10, 14, 16, 18, 22, and 24 of the present patent application, Applicant respectfully submits that it would not have been obvious for one having ordinary skill in the art to have used the applied prior art references to reach the claimed invention. Hence, a rejection of the claims cannot be based upon the cited prior art to establish a *prima facie* case of obviousness. Therefore, a rejection of the claims under 35 U.S.C. § 103(a) has been shown to be insupportable in view of the cited prior art, and the claims are patentable over the applied references. Applicant respectfully requests the withdrawal of the rejection of claims 2, 6, 8, 10, 14, 16, 18, 22, and 24.

V. 35 U.S.C. § 103(a)–Obviousness–*AAPA in view of Zubeldia, Grimmer, and de Silva*

The Office action has rejected claims 4, 12, and 20 under 35 U.S.C. § 103(a) as unpatentable over Applicant's Admitted Prior Art (AAPA) in view of Zubeldia, Grimmer, and de Silva et al.. This rejection is traversed.

The Office action contains a common rejection of dependent claims 4, 12, and 20. These dependent claims primarily differ with respect to the perspective of an entity that acts on an attribute certificate. Since the Office action has focused on claim 4 as representative of these dependent claims, Applicant

provides a rebuttal of the rejection with respect to claim 4 while asserting that the arguments that are provided in support of the patentability of dependent claim 2 are applicable to dependent claims 12 and 20.

The Office action on page 5 states that "AAPA as modified does not explicitly disclose wherein the first locator is stored within an X.509 extension within the attribute certificate." The rejection then states: "However, de Silva discloses the extension is used to store related certificates and serial numbers (de Silva: figure 3 and column 5 lines 15-41 and column 6 line 56-column 7 line 5)." Assuming *arguendo* that de Silva et al. discloses the feature as argued by the rejection, Applicant notes that Zubeldia fails to disclose a locator that identifies a location of a public key certificate of an issuing authority for the attribute certificate, as recited in claim 1 from which claim 4 depends. Since Zubeldia does not disclose a locator, it is irrelevant whether an argument for the inclusion of a locator in an extension of a digital certificate can be made based on the disclosure of de Silva et al. as argued by the rejection. Since Zubeldia does not disclose the claimed feature, notwithstanding the argument in the rejection, it is not possible to combine the teachings of Zubeldia and de Silva et al. to reach the present patent application, notwithstanding the argument in the rejection to the contrary. Again, Applicant asserts that the rejection is deficient for not presenting a *prima facie* case of obviousness with respect to dependent claim 4.

With respect to claims 4, 12, and 20 of the present patent application, Applicant respectfully submits that it would not have been obvious for one having ordinary skill in the art to have used the applied prior art references to reach the claimed invention. Hence, a rejection of the claims cannot be based upon the cited prior art to establish a *prima facie* case of obviousness. Therefore, a rejection of the claims under 35

U.S.C. § 103(a) has been shown to be insupportable in view of the cited prior art, and the claims are patentable over the applied references. Applicant respectfully requests the withdrawal of the rejection of claims 4, 12, and 20.

VI. 35 U.S.C. § 103(a)–Obviousness–*Farrell in view of de Silva and Zubeldia*

The Office action has rejected independent claim 25 under 35 U.S.C. § 103(a) as unpatentable over Farrell et al., "An Internet Attribute Certificate Profile for Authorization", IETF RFC draft-ietf-pkix-ac509prof-05.txt, 08/2000, and further in view of de Silva et al. and Zubeldia. This rejection is traversed.

The Office action on page 6 states that "Farrell does not explicitly disclose wherein the extension comprises a locator identifying a location of a public key certificate of an issuing authority for the attribute certificate." The rejection then states: "However, de Silva discloses the extension is used to store related certificates and serial numbers (de Silva: figure 3 and column 5 lines 15-41 and column 6 line 56-column 7 line 5)." Assuming *arguendo* that de Silva et al. discloses the feature as argued by the rejection, Applicant notes that Zubeldia fails to disclose a locator that identifies a location of a public key certificate of an issuing authority for the attribute certificate, as recited in claim 25.

More specifically, the rejection states:

> Farrell as modified does not explicitly disclose that issuing authority certificate can be obtained through locator. However, Zubeldia discloses issuing authority certificate can be obtained from a certification repository and the repository is accessed through unique ID.

As argued above at length, Zubeldia fails to disclose the claimed feature of a locator that identifies a location of a public key certificate of an issuing authority for the attribute certificate. In addition, Zubeldia cannot be modified to include

the claimed feature. Since Zubeldia does not disclose nor suggest the locator of the present invention, it is irrelevant whether an argument for the inclusion of a locator in an extension of a digital certificate can be made based on the disclosure of de Silva et al. as argued by the rejection. Since none of the applied prior art references disclose the claimed feature, notwithstanding the argument in the rejection, it is not possible to combine the teachings of Farrell et al., Zubeldia, and de Silva et al. to reach the present patent application, notwithstanding the argument in the rejection to the contrary. Applicant asserts that the rejection is deficient for not presenting a *prima facie* case of obviousness with respect to independent claim 25.

With respect to claim 25 of the present patent application, Applicant respectfully submits that it would not have been obvious for one having ordinary skill in the art to have used the applied prior art references to reach the claimed invention. Hence, a rejection of the claim cannot be based upon the cited prior art to establish a *prima facie* case of obviousness. Therefore, a rejection of the claim under 35 U.S.C. § 103(a) has been shown to be insupportable in view of the cited prior art, and the claim is patentable over the applied references. Applicant respectfully requests the withdrawal of the rejection of claim 25.

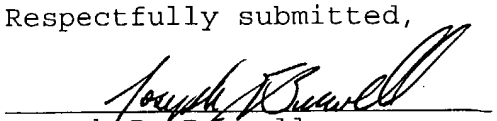
VII. Conclusion

It is respectfully urged that the present patent application is patentable, and Applicant kindly requests a Notice of Allowance.

For any other outstanding matters or issues, the examiner is urged to call or fax the below-listed telephone numbers to expedite the prosecution and examination of this application.

DATE: September 7, 2004

Respectfully submitted,



Joseph R. Burwell
Reg. No. 44,468
ATTORNEY FOR APPLICANT

Law Office of Joseph R. Burwell
P.O. Box 28022
Austin, Texas 78755-8022
Voice: 866-728-3688 (866-PATENT8)
Fax: 866-728-3680 (866-PATENT0)
Email: joe@burwell.biz